MY WEIRD PROMPTS

Podcast Transcript

EPISODE #287

The Chain of Custody: Proving Reality in a Post-Truth Era

Published January 23, 2026 • Runtime: 20:21

https://myweirdprompts.com/episode/digital-forensics-chain-custody/

EPISODE SYNOPSIS

In this episode of My Weird Prompts, Corn and Herman Poppleberry dive into the high-stakes world of digital forensics and the legal mechanics of "truth." As generative AI makes deepfakes indistinguishable from reality, the bar for admissible evidence has shifted from simple recordings to rigorous chains of custody. The brothers explore how tools like ProofMode, the C2PA standard, and WORM (Write Once, Read Many) storage can protect individuals in disputes against bad actors. From cryptographic hashes to AWS S3 Object Lock, learn the technical steps required to turn a simple audio file into a tamper-proof legal shield. Whether you're dealing with a difficult landlord or navigating professional high-stakes meetings, this episode provides a practical roadmap for verifying reality in an increasingly digital world.

DANIEL'S PROMPT

Daniel

"Herman and Corin, I’d like to discuss digital forensics and the chain of custody. In some jurisdictions like Israel, using digital voice recorders for high-stakes meetings—such as with a landlord—is a vital legal protection, even though it impacts privacy. I've found tools like ProofMode, EEVID, and specialized hardware cameras that help ensure digital evidence is tamper-proof and admissible in court. Proving the chain of custody is essential to prevent evidence from being ruled inadmissible. What are some practical steps for gathering evidence while maintaining a proper chain of custody? Specifically, can you explain 'WORM' (Write Once, Read Many) media and the role of certifiable, tamper-free cloud storage in digital forensics?"

TRANSCRIPT

Corn

Hey everyone, welcome back to My Weird Prompts. I am Corn, and I am joined as always by my brother.

Herman

Herman Poppleberry, at your service. It is a beautiful day here in Jerusalem, even if the air is a bit crisp.

Corn

It really is. And you know, living here with our housemate Daniel, we get into some pretty deep conversations over coffee. He actually sent us a fascinating audio prompt this morning that got me thinking about the line between privacy and protection.

Herman

Oh, I heard it. Daniel was diving into the world of digital forensics and the legal side of recording high-stakes meetings. It is a topic that feels more relevant every single day, especially with how good generative media has become lately.

Corn

Exactly. He was talking specifically about the legal landscape here in Israel, where one-party consent for recording is the standard. But he pushed it further than just hitting record on a phone. He wanted to know about the chain of custody, tamper-proof hardware, and this concept of W O R M media.

Herman

It is a brilliant rabbit hole. Most people think that just having a recording is enough to win a case, but in twenty twenty-six, the bar for evidence is so much higher. If you cannot prove the file has not been touched from the second it was created until the second it hits the courtroom, you are in trouble.

Corn

Right, and that is what we are tackling today. This is episode two hundred eighty-three, and we are going deep into the mechanics of digital truth. How do you gather evidence that actually holds up when someone claims it is a deepfake or a manipulated file?

Herman

I love this. It connects so well to what we talked about last week in episode two hundred eighty-two regarding surveillance tech, but this is the defensive side. This is about the average person protecting themselves against bad actors, like a landlord acting in bad faith.

Corn

So, let us start with the basics of that legal context. In a one-party consent jurisdiction like Israel, you can record a conversation you are a part of without telling the other person. But Herman, I heard there were some recent changes to the privacy laws here?

Herman

You have a sharp ear, Corn. Amendment thirteen to the Privacy Protection Law went into effect last year, in January of twenty twenty-five. While it did not scrap the one-party consent rule for recordings, it significantly ramped up the requirements for how you handle and store that data, especially if it contains sensitive information. Admissibility is now a much steeper hurdle.

Corn

Which brings us to the chain of custody. Daniel mentioned this in his prompt. Can you break down what that actually looks like in a digital sense?

Herman

Think of the chain of custody like a baton in a relay race. You need to be able to show exactly who had that baton at every single moment. In digital forensics, the chain of custody starts at the moment of capture. You need to document the device used, the software version, the exact time, and most importantly, the cryptographic hash of the file the moment it was finished.

Corn

A cryptographic hash. We have touched on this before, but for anyone who missed those episodes, that is basically a digital fingerprint, right?

Herman

Precisely. Usually, we use an algorithm like S H A two hundred fifty-six. It takes a file and turns it into a fixed string of characters. If you change even one single bit in that audio file, the hash will look completely different. So, if you record a meeting with your landlord and immediately generate a hash, you can prove later that the file you are showing the court is the exact same one you recorded.

Corn

But here is the problem I see. If I record it on my phone, and then five minutes later I run a hash, the opposition could argue that I had five minutes to run it through an A I voice changer. How do we close that gap?

Herman

That is where the specialized tools Daniel mentioned come in. Tools like ProofMode, which comes from the Guardian Project. ProofMode is fascinating because it does not just record the audio. It captures a massive amount of metadata at the same time—G P S coordinates, cell tower I Ds, and even sensor data from the phone's accelerometer.

Corn

Wait, why would you need the accelerometer data for an audio recording?

Herman

Because it proves the phone was actually in your hand or on a table at that location. It makes it nearly impossible to claim the audio was fabricated in a studio later. ProofMode bundles all that into a cryptographically signed zip file. It uses the C two P A standard—that stands for the Coalition for Content Provenance and Authenticity. It creates a digital seal of authenticity the very millisecond the recording stops.

Corn

That is incredible. It is like bagging and tagging evidence at a crime scene, but the phone does it automatically. I remember we discussed something similar in episode one hundred fifty-one, but applying it to a landlord dispute is a very practical, real-world use case.

Herman

It really is. And Daniel also mentioned hardware cameras. This is huge right now. Sony and Leica have fully integrated Content Credentials into their latest bodies, like the Sony Alpha one Mark two and the Alpha nine Mark three. They even use three-dimensional depth information from the sensor to prove the camera was looking at a real physical person and not just a high-resolution screen.

Corn

I imagine that is going to be the standard for all journalism and legal work soon. If you do not have a signed file, it will be assumed to be A I-generated.

Herman

I think you are right. We are moving into a post-truth era where the default assumption is that everything is fake. The only way to prove reality is through these cryptographic anchors.

Corn

So, let us talk about W O R M media. Daniel asked about this specifically. Write Once, Read Many. Is that still a thing in the age of the cloud?

Herman

It is actually more important now than ever. In a professional forensics context, the real power is in W O R M-compliant cloud storage. Amazon Web Services has a feature called S three Object Lock.

Corn

How does that work? If it is in the cloud, surely an administrator could just delete it?

Herman

Not in Compliance Mode. When you put a file into an S three bucket with Object Lock in Compliance Mode, even the root administrator of the account cannot delete or modify that file until the retention period expires. You could set it for five years, and for those five years, that file is effectively carved in stone. Not even a hacker who steals your credentials can get rid of it.

Corn

That is a powerful piece of the chain of custody. If you record an interaction using ProofMode, and it immediately uploads to a W O R M-configured cloud bucket, you have a perfect, untamperable record. You can tell a judge, look, this was recorded at ten fifteen A M, it was signed by my device, and it was locked in this cloud storage by ten sixteen A M. There was no window of opportunity for me to manipulate it.

Herman

Exactly. You are removing the human element of trust and replacing it with mathematical certainty. For someone in a high-stakes situation, like a tenant facing an illegal eviction, that kind of evidence is a shield.

Corn

I want to push on the privacy aspect for a second, though. Daniel mentioned that this impacts privacy. Even if it is legal, there is a social cost to this, right?

Herman

It is a difficult balance, Corn. On one hand, you have the right to protect yourself from lies and gaslighting. On the other, you have the chilling effect where people are afraid to speak freely. But in the context Daniel brought up, a landlord-tenant meeting, there is a power imbalance. Usually, the person with more power has less to fear from the truth. These tools level the playing field.

Corn

That is a fair point. It is less about spying and more about creating an objective record. But what about the technical hurdles? If I am a regular person, how do I actually set up a certifiable, tamper-free cloud storage?

Herman

It is getting easier. There are services now that act as an intermediary. You use their app, and they handle the back-end W O R M storage and hashing. But if you want to be truly D I Y, you can set up an A W S account, create a bucket with Object Lock enabled, and use an A P I to push your files there. It takes about an afternoon of tinkering.

Corn

I think that is a great practical takeaway for our listeners. If you are entering a situation where you think you might need legal protection, do not just rely on your voice memo app. Take the time to look into something like ProofMode. It is free, it is open-source, and it provides that extra layer of metadata that makes your evidence much harder to dismiss.

Herman

And if you are really serious, look into E-E-V-I-D for emails. Daniel mentioned that one too. It stands for Evidence-Certified Email. It basically acts as a digital registered letter. It tracks when the email was sent, when it was opened, and it provides a certified P D F that proves the content of the message. They even offer a five-year storage guarantee for your receipts.

Corn

It is amazing how much of our lives are now lived in these digital spaces where we have to constantly prove we are telling the truth. I remember back in episode two hundred seventy-nine, we talked about private intelligence and how they use these same tools to verify their sources. It is the same tech, just scaled down for personal use.

Herman

It really is. The world is getting more complex, and the tools to navigate it are getting more sophisticated. But at the end of the day, it all comes back to that one concept: the chain of custody. If you can show the path of the data, you can show the truth of the event.

Corn

You know, I was reading a paper recently about the second-order effects of this kind of ubiquitous recording. One of the points they made was that it might actually lead to more honest behavior in professional settings. If a landlord knows that there is a high probability that a meeting is being recorded with tamper-proof technology, they are much less likely to make illegal threats.

Herman

It is the Hawthorne Effect, right? People change their behavior when they know they are being observed. In this case, it is a forced accountability. I think it is a net positive for society, even if it feels a bit dystopian at first glance. We are moving from a world of reputation-based trust to a world of verification-based trust.

Corn

Trust, but verify. The old saying has never been more literal. Now, Herman, let us get into the weeds of the W O R M media again. You mentioned Compliance Mode versus Governance Mode. What is the difference there?

Herman

Oh, it is a huge distinction. Governance Mode is like a soft lock. It prevents most users from deleting a file, but someone with special permissions, like a senior administrator, can still override it. This is useful for corporate settings where you might need to fix a mistake. But for legal evidence, you want Compliance Mode. In Compliance Mode, nobody can override the lock. Not even the person who created the account. Not even Amazon’s support staff. Once that file is in there, it is stuck until the timer runs out.

Corn

That is the key, isn't it? To make the evidence admissible, you have to prove that even you, the person presenting it, could not have changed it. It removes the bias.

Herman

Exactly. A judge looks at that and sees a system where the user has intentionally given up control to preserve the integrity of the record. That carries a lot of weight.

Corn

So, if someone is listening to this and they are in a dispute right now, what are the three most practical steps they can take today?

Herman

Step one: Download ProofMode. It is available for Android and iPhone. Start using it for any interaction that feels high-stakes. Step two: If you are communicating via email, use a service like E-E-V-I-D to get a certified delivery receipt. And step three: If you can, set up a simple W O R M-enabled cloud bucket. If that feels too technical, at the very least, send a hash of your recording to a third party or use a blockchain-based timestamping service to create a public receipt of your evidence.

Corn

This has been a really enlightening discussion. I think Daniel really hit on something important here. It is not just about the tech; it is about the shift in how we handle truth and accountability in our daily lives.

Herman

It really is. And I am glad he sent it in. It is always fun to nerd out on the intersection of law and technology, especially when it has such a direct impact on how we live here in Jerusalem.

Corn

Well, I think we have covered a lot of ground today. From the legalities of one-party consent to the cryptographic nuances of W O R M storage. If you have found this useful, or if you have your own weird prompts you want us to explore, please get in touch at myweirdprompts.com.

Herman

And while you are there, you can check out all our past episodes. We love seeing the feedback from our regular listeners. It makes those late-night research sessions worth it.

Corn

Absolutely. Well, I think that is a wrap for today. Thanks to Daniel for the prompt, and thanks to all of you for listening. Until next time, stay curious and keep verifying.

Herman

Take care, everyone. See you in episode two hundred eighty-four!

Corn

Bye everyone!

Herman

Bye!